CAAG Projects

Project report: **07/05/2019**
Project presentation: **25/06/2019**

The following projects are supposed to be worked out throughout the semester. Every project group should hand in a short paper and a program plus some examples. For the programs you can use any computer algebra system that does not directly deliver all tasks which are asked.

1 Project Bézout's Theorem

In [1] is given an alternative way of proving Bézout's Theorem.

- Analyze the paper and explain the results and the reasoning in your own words.
- Implement the proposed algorithm to compute intersection points of affine plane curves.

2 Project Parametrizing quartic curves

Consider an irreducible curve $\mathcal{C}$ of degree 4 in the affine plane over $\mathbb{C}$.

- Check whether $\mathcal{C}$ has only ordinary singularities and compute its genus in the affirmative case.
- Suppose that $\mathcal{C}$ is of genus zero (i.e., either 1 triple point or 3 double points). Determine a rational parametrization of $\mathcal{C}$ as it is described in the lecture notes
  a) by lines through the triple point of $\mathcal{C}$.
  b) by conics through the double points and a given rational curve point P.

3 Project Elliptic curves

Let $\mathcal{C}$ be a cubic with a rational point P. In [2] is described a way of defining a group action on $\mathcal{C}$.

- Describe the definition of the group action and its properties in detail.
- Implement the performance of the group action and the scalar multiplication.
- Explain how this can be used in cryptography and give some examples of encoding and decoding a message.

Literatur

[1] J. Hilmar, and C. Smyth. Euclid Meets Bézout: Intersecting Algebraic Plane Curves with the Euclidean Algorithm *The American Mathematical Monthly*, 117(3):250–260, 2010.

[2] J.H. Silverman, and J. Tate *Rational Points on Elliptic Curves*. Springer Verlag, New York, 1992.